## Large-scale databases and interoperability in migration and border policies

BROUWER, Evelien

***published in***
European Public Law
2020

# Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection

Evelien BROUWER*

*In the EU, different measures have been adopted with regard to the storage and exchange of personal data of third-country nationals for external border controls. Large-scale databases and risk assessment are used to facilitate the entry of those considered as 'bona fide travelers' and to identify those considered as a risk of irregular migration or security threat. The purposes of existing databases have been gradually extended, blurring the line between the objectives of immigration control and security and law enforcement. Emphasizing the non-discriminatory approach of data protection and applying criteria from the case-law of the Court of Justice of the European Union (CJEU), this contribution questions the legitimacy of these measures from the perspective of the principles of necessity and proportionality, purpose limitation, and the prohibition of automated-decision making.*

**Keywords:** large-scale databases, interoperability, biometrics, third-country nationals, non-discrimination, data protection, necessity and proportionality, purpose limitation, automated decision-making

## 1 INTRODUCTION

> *The successful elimination of internal frontiers will of course accentuate in a symbolic way (and in a very real sense too) the external frontiers of the Community [ … ] In one way, the more that these external borders are accentuated, the greater the sense of internal solidarity [ … ] in the very concept of European citizenship a distinction is created between the insider and the out-sider that tugs at their common humanity.*[1]

In the EU, different mechanisms have been set up to store and exchange personal data on third-country nationals, both for migration and security control purposes. These measures were in the first place a response to the terrorist attacks in the United States of America of 9 September 2001 and in Europe, in Barcelona (2004) and London (2005). At the EU summit in the Hague in 2004, the heads of governments, underlined the importance of further cooperation and data exchange within the Area of Freedom, Security and Justice (AFSJ), proposing the 'principle of availability' as basis for such

* Vrije Universiteit Amsterdam. Email: e.r.brouwer@vu.nl.

1 J. Weiler, *Thou Shall Not Oppress a Stranger: On the Judicial Protection of the Human Rights of Non-EC Nationals – A Critique*, 3 Eur. J. Int'l L. 65 and 68 (1992).

Brouwer, Evelien. 'Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection'. *European Public Law* 26, no. 1 (2020): 71–92.

cooperation.[2] Since then, this goal of availability or multiple use of personal information has been in particular incorporated in EU border and migration policies. As a response to the increase of asylum seekers travelling to the EU between 2014 and 2016, and terrorist attacks in Paris (2015), Brussels (2016), and other European cities, the EU legislator developed or proposed different measures dealing with data processing for the purpose of border and migration control. In this 'digitization of borders' combined with the politicization of border management, the status of foreigner became more and more the equivalent to 'security risk'.[3] This has resulted in several measures of centralized data collection and surveillance measures with regard to third-country nationals, while comparable measures have not been adopted with regard to Member States' nationals or EU citizens. Dealing with data processing in the field of migration and border control, the EU legislator established itself as a 'very hungry caterpillar'.[4] Additional information tools, such as Entry-Exit System (EES), European Travel and Authorization System (ETIAS), European Criminal Records Information System- Third Country Nationals (ECRIS-TCN), and the Regulation on interoperability have been adopted without prior evaluation of the use and effectiveness of existing databases and mechanisms of data sharing. Furthermore, law enforcement authorities and internal security agencies gained further access to data on third-country nationals.

This contribution submits that these measures may result into new forms of 'digital entry bans' against which it is difficult to invoke effective legal remedies. The use of Schengen Information System (SIS) alerts on return decisions and entry bans, the sharing of data on national criminal records via ECRIS-TCN, and the increasing use of profiling and risk-assessment, may hamper the possibility of individuals to effectively rebut the legitimacy of immigration decision-making. I will advocate the need of revitalizing the non-discriminatory approach in data protection law, based on the rights to privacy and data protection in Articles 7 and 8 of the Charter on Fundamental Rights (CFR), taking into account the new EU data protection regime and relevant criteria of the CJEU in more recent case law.

To understand the scope of data processing in the field of migration and border control, I will provide in the next two sections, a general overview of the existing large-scale databases (section 2) and new measures adopted between 2017 and 2019 (section 3). In section 4, I will address the right to data protection law and case-law of the CJEU, focusing in particular on the purpose limitation

---

2 The Hague Programme on strengthening freedom, security and justice in the European Union, *OJEU* C53, 3 Mar. 2005, at 1.

3 Dennis Broeders & James Hampshire, *Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe*, 39(8) J. Ethnic & Migration Stud. 1201–1218 (2013).

4 Referring to the title of the children's picture book, Eric Carle, The Very Hungry Caterpillar (first published 1969).

principle, the 'necessity and proportionality test', and the prohibition of 'automated decision-making'. Some closing remarks will be made in section 5.

## 2 BORDER CONTROL AND EU LARGE-SCALE DATABASES

### 2.1 Schengen information system

When the SIS became operational on 26 March 1995, the system was used by seven States: Belgium, the Netherlands, Luxembourg, France, Spain, Portugal and Germany. In 2019, the SIS is used by twenty-six states, including EU and non-EU Member States. At the beginning of the negotiations on the SIS, the participating states mainly focused on the use of this system for security and police purposes. According to a draft text of 1988, the purpose of the information system was to 'guarantee public order and security and fight criminality on the territories of the Contracting Parties, with the help of the information received by this system'.[5] Later, at the initiative of the Dutch government, this purpose was extended to the application of immigration law, including provisions on visa applications procedures and free movement of persons. SIS II includes the following categories of persons: persons wanted for arrest for extradition purposes (on the basis of the European Arrest Warrant (EAW) Framework Decision, see below); missing persons, persons who are wanted by judicial authorities during the course of a prosecution (for example as witness); and, central to our contribution, third-country nationals to be refused entry or stay to the Schengen territory. Furthermore, SIS contains alerts on persons reported for the purpose of discreet surveillance or specific checks, following indications that a person 'intends to commit, or is committing numerous and extremely serious offences' or 'where an overall evaluation of the person', 'gives reasons to suppose that he or she 'will also commit extremely serious offences in future' .[6] Since SIS became operational, the majority of persons reported into SIS concerned third-country nationals reported for the purpose of refusal of entry and between 1999 and 2004 this percentage of 'inadmissible aliens' was about 85–90% of the total number of persons reported in SIS. This relative high percentage however gradually dropped after the entry into force of the EAW Framework Decision in 2004. In 2018, SIS II contained 935,497 alerts on persons of which 504,590 alerts (53.9%) on third-country nationals reported for the purpose of refusal of entry or stay.[7]

The so-called second generation SIS was established on the basis of Decision 2007/533 and Regulation 1987/2006, extending its users and allowing for new functions.[8] On

---

5 88 (SCH/1 (88) 7) 27 Oct. 1988, para. 2.2.

6 Article 36 Council Decision 2007/533 of 12 June 2007, OJ L 205, 7.8.2007.

7 SIS II Statistics 2018, https://www.eulisa.europa.eu/Publications/Reports/SIS%202018%20statistics.pdf, published by euLISA 2019 (accessed 11 Dec. 2019).

8 SIS II Regulation 1987/2006 *OJ* L 381 of 28 Dec. 2006 and Decision 2007/533 *OJ* L 205 of 7 Aug. 2007.

the basis of the SIS II Regulation 1987/2006, the criteria to report a third-country national as 'inadmissible', or with purpose of refusal of entry to the Schengen territory, in SIS II remained almost the same as provided in Article 96 of the Convention on the Implementation of the Schengen Agreement (CISA). First, a person may be registered, if he or she is considered as a threat to public policy or public security or national security, for example if the person is convicted by a Schengen state for a crime punishable with a deprivation of liberty for at least one year, but also if he or she is the object of a restrictive measure intended to prevent entry into or transit through the territory of Member States, including those implementing a travel ban issued by the Security Council of the United Nations.[9] Second, a SIS alert for the refusal of entry will be entered into SIS II if the third-country national has been subject to a decision of expulsion, refusal of entry, or removal. This includes entry bans issued on the basis of the Return Directive 2008/115.[10] The use of SIS is thus based on mutual recognition of, and trust in, national decisions of the other state submitting the alert. On the basis of the Schengen Borders Code and Visa Code, entry respectively the issuing of a short-term visa must be refused to a person who is registered into SIS II for the purpose of refusal of entry.[11] Articles 21 and 24 (1) Regulation 1987/2006 added the requirement of a proportionality test and an individual assessment before entering an alert on third-country nationals in SIS II. Until now, the CJEU did not address the legitimacy or proportionality of SIS alerts itself. However, both with regard to an EAW and alerts for the purpose of refusal of entry or stay in SIS, the CJEU underlined the obligation of Member States to check whether their execution does not violate fundamental rights of the person concerned.[12]

### 2.1[a] *Amendments 2018: Storage of DNA and Biometrics and Extended Categories of 'Entry Bans'*

In June 2018, three Regulations were adopted extending the use of SIS II further and replacing the aforementioned Directive 2007/533 and Regulation 1987/2006.[13] They include Regulation 2018/1862 on the use of SIS within the field of police

---

9 On the basis of the EU Council of 27 Dec. 2001 on the *Decision Establishing the List Provided for in Article 2 (3) of Council Regulation 2580/2001 on Specific Restrictive Measures Directed Against Certain Persons and Entities with a View to Combating Terrorism* and the (much longer) list in the Annex of the *Common Position 2001/931 on the Application of Specific Measures to Combat Terrorism* and *Council Decision 2001/927, OJEU* L 344, 28 Dec. 2001 and *OJEU* L 139/4 and L 139/9, 29 May 2002.

10 In accordance with the Return Directive, Member States must adopt a return decision to irregularly staying third-country nationals. If no period of voluntary return is granted, this return decision may be followed by an entry ban. Until recently, this reporting of entry bans into SIS had no explicit legal basis, but was only mentioned in recital 18 of the Return Directive *OJEU* L 348, 24 Dec. 2008. As we will *see* below, an amendment of Art. 24 SIS II Regulation 1987/2006 now provides in a legal basis.

11 Regulation 399/2016 *OJEU* L 77, 26 Mar. 2016 resp. Regulation 810/2009, *OJ* L 243, 15 Sept. 2009.

12 CJEU C-404/15, *Aranyosi*, 5 Apr. 2016, C-503/03, *Commission v. Spain*, 31 Jan. 2006.

13 *OJEU* L 312, 7 Dec. 2018.

and judicial cooperation; Regulation 2018/1861 SIS II on the use of alerts on third-country nationals for border checks; and Regulation 2018/1860 providing for the (obligatory) storage of return decisions into SIS. The amendments will become binding on the basis of an implementing decision of the Commission which must be adopted no later than 21 December 2021.[14]

Regulation 2018/1862, dealing with the use of SIS for judicial and law enforcement purposes, provides for the possibility to include DNA for missing children (Article 22.1 (b)) and for preventive alerts to be issued, subject to procedural safeguards, in the case of potential parental abduction (Articles 32 and 33). Furthermore, the amended rules provide for the storage of dactylographic data not related to persons subject to an alert in SIS II. This storage allows the identification of so-called 'unknown wanted persons' (Articles 40–42), or according to the explanatory memorandum, to enable 'the fingerprints of an unknown perpetrator to be uploaded into SIS so that he or she can be identified as wanted, if encountered in another Member State'. This storage of these data requires that first, it is established to 'a high degree of probability' that they belong to the perpetrator of a serious crime or act of terrorism, and second, the competent authorities cannot establish the identity of the person by using any other national, European or international database.

Regulation 2018/1861 on the use of SIS for the purpose of border controls maintains the two different categories included in Article 24 (1) (a) and (b) of the current SIS II Regulation: first, SIS alerts based on national administrative and judicial decisions related to the fact that the presence of that third-country national would pose a threat to public policy, to public security or to national security, and, second, alerts based on entry bans in accordance with the Return Directive. Article 24 (2) of the new Regulation adds another category of SIS alerts for the purpose of public policy or security, namely third-country nationals 'circumventing national law on entry or stay'. The open formulation of this criterion extends the already wide discretion of national authorities to report third-country nationals for the purpose of refusal of entry into SIS. In accordance with 24 (1) (b) Regulation 2018/1861, it becomes mandatory for Member States to enter a SIS alert following an entry ban. Furthermore, even in the situation a return decision is not followed by an entry ban, Regulation 2018/1860 provides that every return decision on the basis of the Return Directive must be reported into SIS, for the purpose of 'verifying that the obligation to return has been complied with and of supporting the enforcement of the return decisions'. Regulation 2018/1861 makes the use of

[14] *See* respectively Art. 79 Regulation 2018/1862 and Arts 20 Regulation 2018/1860 and 66 (2) Regulation 2018/1861.

biometric identification obligatory if the identity of the person at stake cannot be ascertained in another way.

The goal of reporting alerts on third-country nationals for the purpose of refusal of entry or stay into SIS was first and foremost border and immigration control.[15] Gradually however, the SIS has been developed into an investigation tool, which use is enhanced by the possibility to check the availability of a hit in SIS II on the basis of biometric data and by allowing access to judicial and police authorities to data on third-country nationals. Article 27 Regulation 1987/2006 already provided access to 'authorities responsible for the identification of third-country nationals' for the purpose of border and police and customs checks and to national judicial authorities. Articles 34 of Regulation 2018/1861 and 17 of Regulation 2018/1860 extended this access for the prevention, detection, investigation, or prosecution of terrorist offences or other serious criminal offences, and for security checks on third-country nationals applying for asylum. Furthermore, on the basis of the new rules, the European Border Coast Guard (EBCG) but also Europol will have access to SIS alerts on third-country nationals.[16]

### 2.2 Eurodac

The second EU large-scale database on third-country nationals is Eurodac. This first 'Automated Fingerprint Identification System' (AFIS) in the EU, includes fingerprints of asylum seekers and of third-country nationals crossing the external borders of Member States irregularly. Eurodac is operational since 15 January 2003 on the basis of Regulation 2725/2000, meanwhile replaced by Regulation 603/2013.[17] Its purpose is to facilitate the application of the Dublin Regulation to determine the Member State responsible for an application for international protection within the EU. Whereas the implementation of 'Dublin' did not result in a more effective and solidary response to asylum applications in the EU, the necessity of central and long-term storage of biometrics of every person applying for international protection may be questioned as well.[18]

---

15 In 2017, entry or stay would have been refused to 150,000 persons on the basis of information in SIS. European Commission, Press release 12 June 2018 following the agreement between the Council and the European Parliament on the Commission proposals to strengthen the Schengen Information System, 18/4133, http://europa.eu/rapid/press-release_STATEMENT-18-4133_en.htm.

16 Articles 35 and 36.

17 *OJEU* L 180, 29 June 2013.

18 M. Di Filippo, *From Dublin to Athens: A Plea for Radical Rethinking of the Allocation of Jurisdiction in Asylum Procedures*, International Institute of Humanitarian Law. Policy Brief (2016), https://www.researchgate.net/publication/292608372_From_Dublin_to_Athens_A_Plea_for_a_Radical_Rethinking_of_the_Allocation_of_Jurisdiction_in_Asylum_Procedures; E. Guild et al., *Enhancing the Common European Asylum System and Alternatives to Dublin*, European Parliament, *Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs*, PE 519.234 (2015b),

Nevertheless, instead of evaluating the use and effects of Eurodac first, Eurodac has been made accessible since 20 July 2015 for law enforcement purposes on the basis of Regulation 603/2013. Articles 20 and 21 provide access to national 'designated authorities' respectively Europol. After critical comments on the first draft by different organizations including the European Data Protection Supervisor (EDPS), the legislator added in Article 20 two sets of conditions to be fulfilled before access to national law enforcement authorities is allowed. Before submitting a reasoned electronic request for comparison with Eurodac data, the authorities should first check their national fingerprint databases, data systems of other Member States by applying the Prüm framework (Decision 2008/615), and the Visa Information System (VIS). Only if the comparison with these databases does not lead to the identification of the data subject, access to Eurodac is allowed under a second, cumulative set of conditions. First, access should be necessary for the prevention, detection, or investigation of terrorist offences or of other serious criminal cases. Second, this access must be necessary in a specific case and third, there should be 'reasonable grounds to believe that comparison will contribute to the prevention, detection, or investigation of the crime'. The same limitations apply to Europol, except that Article 21 does not mention specific databases to be checked on beforehand, but Article 21 (1) refers to 'any information processing systems that are technically and legally accessible by Europol'.[19] Both categories of data are difficult to be checked in practice, first because of the wide and open definition of the purpose for which comparison with Eurodac is sought (including 'prevention' of terrorist offences and serious crimes), and second because it is unclear how it will be tested in practice whether the designated authority or Europol did check other available databases. Statistics provided by the EU Agency euLISA on the use of Eurodac in 2018 reveal a relatively high number of 'local hits' on the basis of searches by Member State law enforcement authorities.[20] Local hits are produced when the two datasets generating the hit are from the same country. This implies that those searches for law enforcement purposes are in breach of the aforementioned condition for such access, namely that national data sets should be checked first.

---

www.europarl.europa.eu/RegData/etudes/STUD/2015/519234/IPOL_STU(2015)519234_EN.pdf; D. Stevens, *The Humaneness of EU Asylum Law and Policy*, in *The Human Face of the European Union: Are EU Law and Policy Humane Enough?* 248 (N. Ferreira & D. Kostakopoulou eds, Cambridge: Cambridge University Press 2016); ECRE, *AIDA Annual Report 2014/2015* 48 (2015); V. Chetail, *The Common European Asylum System: Bric-à-brac or System?*, in 7 (V. Chetail, P. De Bruycker & F. Maiani eds 2016); M. V. Garlick, *The Dublin System, Solidarity and Individual Rights*, in 170–174 (V. Chetail, P. De Bruycker & F. Maiani eds 2016).

[19] *See* on the data processing powers of Europol and the meaning of purpose limitation: Fanny Coudert, *The Europol Regulation and Purpose Limitation: From the 'Silo Based Approach' to … What Exactly?*, 3 Eur. Data Prot. L. Rev. 313 (2017).

[20] euLISA, *Eurodac Statistics 2018* 16 (Feb. 2019).

A list produced by the European Commission on the authorities having access to Eurodac in accordance with Article 5 (2) Eurodac Regulation for the purpose of law enforcement reveals many differences between the national practices of the thirty-two EU and non-EU Member States having access to Eurodac.[21] It also establishes a very high number of organizations allowed with access: with Member States mentioning only two or four 'designated authorities' (Austria, resp. Greece) to Member States listing between fifty and even more than 200 authorities having access to Eurodac (Belgium, France, Italy).[22]

## 2.3 VIS

The third and largest 'large-scale database' within the EU concerns the VIS, provided in Regulation 767/2008.[23] The primary purpose of VIS is to facilitate (short) visa application procedures on the basis of the Visa Code or Regulation 810/2009 and checks at external borders in accordance with the Schengen Borders Code (Regulation 2016/399). The VIS is operational since 2011 and is currently accessible by twenty-six states (EU and non-EU Member States). This database stores every visa application for the Schengen territory by third-country national which country of origin is listed in the so-called visa list in Regulation 539/2001.[24] In 2017, VIS included over 49 million visa applications and almost forty-two fingerprints sets.[25] Every decision on the visa application, including a visa refusal or the annulment of a visa, will be stored for five years. VIS has been developed from the start as a multipurpose tool, facilitated by the inclusion of biometrics and the definition of additional purposes. These purposes include prevention of visa shopping and ID fraud, the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States, and to facilitate the implementation of the Dublin Regulation in assessing the Member State responsible for asylum application. Finally, also VIS is accessible to designated national authorities and Europol for 'the prevention, detection or investigation of terrorist offences and of other serious criminal offences' in accordance with the rules in Article 3 VIS Regulation.

---

21 See the list of 105 p. 'EU EURODAC List of authorities 191016 Art. 5.2 Eurodac Regulation', submitted by the European Commission after a FOIA request.

22 Lehte Roots, *The New Eurodac Regulation: Fingerprints as a Source of Informal Discrimination*, 5(2) Baltic J. Eur. Stud. 108–129 (2015).

23 *OJEU* L 218 13 Aug. 2008.

24 Council Regulation (EC) No 539/2001 of 15 Mar. 2001, *OJ* L 81, 21 Mar. 2001, at 1, amended several times since 2001.

25 euLISA, *Technical Reports on the Functioning of VIS* (May 2018), https://www.eulisa.europa.eu/Publications/Reports/2018%20VIS%20reports%20-%20Factsheet.pdf.

## 3 NEW MEASURES: EES, ECRIS-TCN, ETIAS, AND INTEROPERABILITY

### 3.1 EES: Adopted in 2017

In 2011, the European Commission published its communication on 'Smart Borders – options and the way ahead'.[26] Two years later, this was followed by the so-called 'Smart Borders package' entailing proposals for an EES and a Registered Traveller Programme (RTP).[27] The aim of these proposals as defined by the Commission, were to facilitate the travelling of so-called bona fide travellers and to ensure security and to prevent irregular immigration, the latter in particular by detecting visa-overstayers. During the negotiations, mainly for cost-efficiency reasons, the proposal for the RTP was withdrawn. The EES proposal received numerous and critical comments. The EDPS addressed both the lack of evidence on the added value and the intrusiveness of these measures for the individual rights of the persons at stake.[28] Despite these comments, the Regulation establishing the EES was adopted by the Council and the European Parliament in November 2017.[29]

The EES is expected to be operational in 2020 and will include information on the entry and exit of each third-country national with the aim to prevent irregular overstay and to protect internal security. The system is meant to facilitate the fast and easy entrance to the EU of so-called 'bona-fide travelers', while at the same time providing information on the cross-border movements and travel history of migrants to immigration and law enforcement authorities. EES will record data on date, time, and place of not only entry and exit of all third-country nationals admitted for a short stay to the EU and who are subject to border checks in accordance with the Schengen Borders Code. Third-country nationals who are family members of EU citizens are not registered into EES, unless they do not carry a residence card in accordance with the Citizenship Directive 2004/38 or a residence permit in accordance with Regulation 1030/2002 on the uniform format for residence permits. The EES will also store data on third-country nationals who have been refused entrance on the basis of the criteria of the Schengen Borders Code. Border guards creating the individual file in EES, will collect four fingerprints of visa-exempt third-country nationals from the age of twelve years. The

---

[26] European Commission, *Smart Borders – Options and the Way Ahead*. Brussels, COM (2011) 680 final, 25 Oct. 2011.

[27] COM (2013) 95, 96, 97.

[28] EDPS, *Smart Borders: Key Proposal Is Costly, Unproven and Intrusive*, Press Release 2013/08 (19 July 2013). *See* a detailed analysis of the proposals in Julien Jeandesbosz et al., *The Commission Legislative Proposals on Smart Borders: Their Feasibility and Costs*, Study on behalf of the European Parliament (LIBE Committee 2013), http://www.europarl.europa.eu/studies.

[29] Regulation 2017/2226 of 30 Nov. 2017, *OJ* L 327, 9 Dec. 2017, at 20. See for the Commission proposal: 2016/0106 (COD).

fingerprints of third-country nationals requiring a visa, are already available via VIS.[30]

As with regard to SIS, VIS and Eurodac, law enforcement authorities and Europol also will have access to EES. Articles 29 and 30 of the EES Regulation provide that 'designated authorities' respectively Europol are entitled to consult EES data in order to prevent, detect, or investigate terrorist offences or other serious criminal cases. According to the conditions in Articles 31–33, this access must be necessary and proportionate in a specific case and there should exist 'evidence or reasonable grounds' that consultation of EES will contribute to the prevention, detection, or investigation of the criminal offences in question. National designated authorities may only have access to EES after a prior search has been conducted in national databases. Finally, the EES Regulation itself, so independent of the Regulation on interoperability described below, provides for 'interoperability' with the VIS. The EU Agency euLISA, responsible for the development and management of the EES, is tasked to develop a 'Secure Communication Channel' between EES and VIS.

### 3.2 ETIAS: Adopted in 2018

On 25 April 2018, the Council and the European Parliament adopted the ETIAS, proposed by the European Commission in 2016 for 'strengthening integrated border management and enhancing internal security'.[31] The ETIAS system, once operational, requires visa-exempt third-country nationals to apply for a travel authorization and to submit personal information into an online application before travelling to the EU.[32] The ETIAS Regulation provides for another centralized database the 'ETIAS Central System' in which personal information on third-country nationals is kept for at least five years. Furthermore, the decision-making on whether or not granting a travel authorization will be based on an extended use of profiling and algorithms, involving the use of the other EU large-scale databases.

The purpose of ETIAS is to prevent the entry of third-country nationals whose presence in the EU would pose a security, illegal immigration, or high epidemic (health) risks. To enable the assessment of these risks and thus whether a person is eligible to enter the EU, three levels of information sorting will be used.

---

30 In Mar. 2019, the European Parliament agreed with a proposal of the Commission, COM (2018) 302, to lower the age of visa applicants who have to provide fingerprints to six years.

31 Regulation 2018/1240 establishing a European Travel Information and Authorization System *OJ* L 236, 19 Sept. 2018. Press Release of the European Council 217/18, 25 Apr. 2018. See for the proposal COM (2016)731, 16 Nov. 2016.

32 ETIAS is comparable to ESTA, the online authorization that EU and other visa-exempt citizens need to fill in prior to traveling to the USA in order to be authorized to travel (for less than three months) as tourists.

First, an automated comparison will take place with national and EU databases, for example to check if travel documents have been reported as stolen, lost or invalidated in SIS or national databases, or if the person has been reported for the purpose of refusal of entry into the SIS. Second, there will be an assessment based on 'ETIAS screening rules' which, according to Article 33 will consist of 'an algorithm enabling the comparison between the data recorded in an application file of the ETIAS Central System and specific risk indicators pointing to irregular migration, security or public health risks. These ETIAS screening rules will be registered in the ETIAS Central System. Third, the personal information of the applicant of the travel authorization will be compared to the 'ETIAS watch list' (Articles 34, 35). This list will consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there is a 'factual indication or reasonable ground, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence'. Member States and Europol may enter information to this ETIAS watch list.

The ETIAS Regulation provides for interoperability between the ETIAS Central System with SIS II, Eurodac, VIS, ECRIS-TCN, and the EES, for the purpose of the automated processing and verification of the application file (Articles 11, 20). According to Article 20, the applications will be automatically processed, after which 'the ETIAS Central System shall examine each application file individually'. If the automated processing does not report any hit, the ETIAS Central System will automatically issue a travel authorization (Article 21). If one or several hits are reported, the ETIAS Central Unit will be consulted and the application will processed manually by the ETIAS National Units of the Member States (Articles 22, 26). The decision on the travel authorization is taken by the ETIAS National Unit of the responsible Member State (Articles 25, 26). Once issued, the travel authorization remains valid for five years. Data will remained stored in the ETIAS Central System for the duration of the authorization, or five years from the last decision to refuse, annul or revoke the travel authorization.

If an application for travel authorization is refused, the applicant will receive a notification by email (Article 38). This notification will include information on the right to appeal and a statement of the grounds of refusal as listed in Article 37 (1) and (2). These refusal decisions will not include substantiated or individualized information, but merely state the category of the grounds of refusal (such as the fact that the person is reported in the SIS for the purpose of refusal of entry, poses a security, illegal immigration, or high epidemic risk). The presence of reasonable and serious doubts as to the authenticity of presented documents or statements of the applicant, may be a ground for refusing travel authorization.

The ETIAS database will be accessible to law enforcement authorities and Europol. Responding to concerns expressed by the EDPS in 2017, this access is only allowed under conditions comparable to those applicable to Eurodac, VIS, and EES.[33]

### 3.3 ECRIS-TCN: Adopted in 2019

The ECRIS-TCN Regulation 2019/816, adopted in April 2019, provides for a centralized system containing information on criminal convictions of third-country nationals.[34] The presented aim of ECRIS-TCN is to supplement the existing decentralized network ECRIS on EU citizens.[35] This latter system is currently used by EU Member States to exchange information on previous convictions on EU citizens as contained in the national criminal record systems.[36] The ECRIS-TCN would ensure the exchange of criminal record information for non-EU citizens and EU-citizens with dual nationality, including the nationality of a third country. According to the Explanatory Memorandum to this proposal, the central processing of information on convicted third-country nationals would be necessary because if Member States currently need information concerning convictions of third-country nationals, they can obtain this information only by sending a so-called 'blanket request' to all Member States, which would be a time-consuming and costly procedure. This problem, according to the explanatory memorandum, does not occur for convicted EU citizens, as each conviction within an EU state of an EU citizen, will always be reported to the Member State of nationality and via ECRIS, national authorities can address the Member State of nationality, if they need information on convictions of EU citizens. Aside from this practical reason to develop a central database of convictions on third-country nationals, the Explanatory Memorandum makes clear that security issues and 'the political stance for a more effective and efficient data exchange in the aftermath of the recent terror attacks in Europe' is one of the objectives of the proposal.[37] Article 1 of the Regulation states that the purpose of the ECRIS-TCN is first, to identify the Member State holding information on previous convictions of third-country nationals and second, to lay down the conditions under which the ECRIS-TCN shall be used by 'central authorities' to obtain such information.[38] According to Article 7, the information stored on previous

---

33 EDPS Opinion 3/2017, on the ETIAS proposal, 6 Mar. 2017, point 51: 'Access to existing and future EU databases by law enforcement authorities and Europol should not become the principle, but rather be allowed in limited cases where the need and proportionality of granting such access is fully justified and demonstrated'.

34 *OJ* L 135, 22 May 2019. *See also* press release, http://europa.eu/rapid/press-release_IP-19-2018_en.htm.

35 COM (2017)344 of 29 June 2017.

36 Framework Decision 2009/315 and Council Decision 2009/316.

37 European Commission on 29 June 2017, SWD (2017) 248 final.

38 'Central authorities' are authorities designated in accordance with Art. 3 (1) of the Framework Decision 2009/315 on the exchange of information extracted from criminal records between EU Member States.

criminal convictions on third-country nationals can be requested for criminal proceedings or for any of the other purposes mentioned in this provision, if provided by national law. These other purposes include security clearances; obtaining a license or permit; employment vetting; vetting for voluntary activities involving contacts with children or vulnerable persons; checks in relation with public contracts and public examinations, but also 'visa, acquisition of citizenship and migration procedures, including asylum procedures'.

This latter purpose means that national immigration and asylum authorities may, if provided by national law, check ECRIS-TCN and may decide to rely on information on criminal records of other Member States.

The ECRIS-TCN will store data on third-country nationals following national decisions related to criminal convictions or prosecutions. This may include criminal convictions of third-country nationals based on violations of national immigration laws. The differences with ECRIS are striking: whereas the ECRIS-TCN provides for the exchange and collection of fingerprints, facial recognition and other possible biometric data of third-country nationals, ECRIS does not include biometrics. And different from ECRIS, the information in ECRIS-TCN will be accessible for Europol, Eurojust and the European Public Prosecutor.

In the evaluation report on ECRIS, the Commission pointed out to significant differences in national criminal law policies with regard to the exchange of information on EU citizens.[39] Amongst others, Member States were found to have different interpretations of the term 'conviction'. Where some Member States exchange data solely on criminal convictions, others would exchange data on non-criminal convictions as well. The Netherlands, for example, processes information not only on non-judicial decisions, but also on pending matters, thus without a conviction. These differences in implementation were not taken into account during the negotiations on ECRIS-TCN. However, the lack of harmonized criteria for storing information on criminal records into ECRIS-TCN, may have consequences for the migration status of the data subjects. As mentioned above, the Regulation allows that ECRIS-TCN will be used in national immigration procedures. Already in its opinion of 2015, the Fundamental Rights Agency (FRA) warned against the risk that ECRIS-TCN would be used for migration purposes to withdraw or refuse issuance or extension of residence permits.[40] Therefore, the FRA proposed to clearly define the system's purpose in a manner that limits the Member State's discretion and to consider an explicit prohibition of using ECRIS-TCN information for immigration law enforcement purposes outside criminal law proceedings. The

[39] COM (2016) 6, 19 Jan. 2016.

[40] FRA, Opinion 1/2015, http://fra.europa.eu/en/opinion/2015/fra-opinion-exchange-information-third-country-nationals-under-possible-system.

FRA also warned against secondary effects from national convictions based on previous irregular entry or stay, which, specifically for refugees and children, would have adversary effects for their integration and protection. The FRA referred to the differentiated practices with regard to criminalization of irregular stay and entry, emphasizing that the use of ECRIS-TCN information thus could lead to different effects, dependent of the laws and practices of Member States. For this reason, the FRA recommended not to process convictions which are related to irregular entry and stay into ECRIS-TCN. In reaction to these concerns, the Commission stated that although the ECRIS-TCN is not meant as a tool for regulating migration, the extent to which criminal record information is processed for other purposes would be 'a matter of national law'.[41] Therefore, limitations to this further use would not be possible in the ECRIS-TCN proposal. This answer illustrates that the Commission implicitly accepts that Member States will use information on criminal records in the ECRIS-TCN for immigration law decisions, even if these decisions are based on the criminal law systems of other Member States.[42]

### 3.4 Regulation on interoperability: Adopted in 2019

Regulation 2019/817 and Regulation 2019/818, adopted on 14 May 2019, establish a framework for the interoperability between EU information systems in the AFSJ.[43] The interoperability of the EU large-scale databases should provide for easier information sharing and 'considerably improve security in the EU, allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat illegal migration'.[44] The interoperability scheme allows national authorities to check whether information on an individual person is recorded in any of the EU databases (VIS, SIS II, Eurodac, the EES, ETIAS, and ECRIS-TCN). This access is based on four mechanisms: first, a European Search Portal (ESP) will serve as a 'message broker' enabling users to search multiple information systems simultaneously, using both biographical and biometric data. Second, the use of a shared biometric matching service (shared BMS) will enable the querying and comparison of biometric data (fingerprints and facial images) recorded in Eurodac, VIS, the future EES, ETIAS and ECRIS-TCN. Third, a common identity repository (CIR) is to be used for the storage biographical and biometric identity data of third-country nationals available from

41 See at 7 of the explanatory memorandum.
42 *See also* Chris Jones, *Disproportionate and Discriminatory: The European Criminal Records Information System on Third-Country Nationals (ECRIS-TCN)*, Statewatch Analysis (Feb. 2019).
43 *OJEU* L 135, 22 May 2019.
44 Proposal for Regulation on interoperability for border and visa purposes 2017/0352 (COD) and the proposal on interoperability for the purpose of police and judicial cooperation, asylum and migration, 2017/0351 (COD).

the aforementioned EU datasystems. Fourth, a multiple-identity detector (MID) will enable to detect multiple identities linked to the same biometric data.

The central objectives of interoperability, as presented by the Commission, are first, to ensure that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have 'fast, seamless, systematic and controlled access' to the information that they need to perform their tasks. Second, it should provide a solution to detect multiple identities linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of *bona fide* persons and combating identity fraud. Third, interoperability of systems will facilitate identity checks of third-country nationals, on the territory of a Member State, by police authorities. And finally, it would 'facilitate and streamline' access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.[45]

Referring to the goal of preserving security in the EU, the Commission implicitly refers to the differentiated treatment between EU citizens and third-country nationals by stating that: 'Whilst not directly affecting EU nationals [ … ], the proposals are expected to generate increased public trust by ensuring that their design and use increases the security of EU citizens'. (emphasis added).[46] According to the Commission, interoperability will not change the purpose, content, or structure of the different EU databases: the relevant identity data would be stored in the CIR but would continue to 'belong' to the respective underlying systems that recorded this data. This assumption has been refuted by the FRA and the EDPS, expressing their concerns about the blurring of the different purposes of each database.[47] As pointed out by the EDPS in Opinion 4/2018, the interoperability regulation in itself creates a new centralized database containing information about millions of third-country nationals, including their biometric data. The consequences of any data breach could seriously harm a potentially very large number of individuals and, according to the EDPS, if 'such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights'. As in the other aforementioned databases, biometrics will be the main tool to facilitate the interoperability to the databases and to check whether or not a person has been registered in one of these databases, with or without knowledge of the data subject.[48]

---

45 Explanatory memorandum, at 3.

46 Explanatory memorandum, stating at 17.

47 EDPS, Opinion 4/2018, 16 Apr. 2018, https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en and FRA, Opinion of 19 Apr. 2018, http://fra.europa.eu/en/opinion/2018/interoperability.

48 E. J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Analysis* 359 (Dordrecht: Springer Science+Business Media, Law, Governance and Technology Series 12, 2013).

### 3.5 Multiplication of borders: Effective remedies

The interlinked use of aforementioned databases, the access to law enforcement authorities to administrative data on third-country nationals, coupled to new technologies of biometrics and surveillance, result in as defined by Trauttmansdorff, a 'multiplication of borders'.[49] The discretionary powers of police and immigration authorities inside the territory and within internal border areas,[50] combined with the possibility to check aforementioned data systems, includes the risk that third-country nationals or those considered to be third-country nationals, will be more often stopped for identification and comparison of their (biometric) data. Consequently, they may be confronted with disproportionate or arbitrary barriers of entry, expulsion, or law enforcement measures.

For third-country nationals, effective remedies against decision-making based on foreign SIS alerts or risk assessment, may be hampered because of two reasons. First, as data sharing is based on the principle of mutual trust, executing Member States will be reluctant to test the lawfulness of entry bans or information from other states. Second, the use of foreign alerts and profiling (including analysis provided by EU agencies, as the European Border and Coast Guard[51]) makes it difficult, if not impossible to trace the source of information resulting in the refusal of entrance or expulsion decision.

## 4 APPLYING THE NON-DISCRIMINATORY APPROACH OF DATA PROTECTION LAW

The following sections will address the aforementioned measures from the perspective of the non-discriminatory application of the right to data protection. The right to data protection is protected in Article 8 CFR and the General Data Protection Regulation (GDPR, Regulation 2016/679) and the Directive 2016/680 dealing with the protection of personal information in the field of law enforcement of 2016 Law Enforcement Directive (LED), applicable as from 25 May 2018.[52] Using relevant criteria developed by the CJEU in its case-law, this section will focus on the principle of necessity and proportionality, purpose limitation, and the prohibition of automated decision-making. Whereas this

---

[49] Paul Trauttmansdorff, *The Politics of Digital Borders*, in *Border Politics* 121 (C. Günay & N. Witjes eds, Springer International Publishing 2017).

[50] Maartje van der Woude en Joanne van der Leun, *Crimmigration Checks in the Internal Border Areas of the EU: Finding the Discretion that Matters*, in *Special Issue on Crimmigration in Europe* 27–45 (Maartje van der Woude, Vanessa Baker & Joanne van der Leun eds, 14(1) Eur. J. Criminology 2017).

[51] *See* Art. 66(4) of the Regulation 2019/817 on interoperability.

[52] Regulation 2016/679 of 27 Apr. 2016, *OJ* 4 May 2016, L 119 repealing Directive 95/46 and the Directive 2016/680, *OJ* 4 May 2016 L 119/89 repealing Decision 2008/977/JHA.

section does not deal separately with the right to private life protected in Articles 8 ECHR and 7 CFR, Article 8 ECHR and case-law of the ECtHR played an important role within the case-law of the CJEU.[53] These rights and principles should be applied indiscriminately to third-country nationals on the basis of Articles 14 ECHR and 21 CFR.[54] This was affirmed by the CJEU in the *Huber* judgment, underlining the non-discriminatory application of the principle of purpose limitation.[55] Whereas this judgment dealt with the (former) Article 12 Treaty Establishing the European Community (TEC), forbidding discrimination on the basis of nationality between EU citizens, the reasoning of the CJEU, prohibiting disproportionate differences in treatment when assessing data processing and the right to data protection, are generally applicable.[56]

### 4.1 The necessity and proportionality test

The right to data protection, applies to everyone within the jurisdiction of the Member States and the EU. Limitations to these rights must observe the general conditions as provided in 52 (1) CFR. This means that any limitation to the right to data protection is provided for by law and respect the essence of those rights and freedoms, subject to the principle of proportionality. Furthermore, the limitation must be necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others'.[57] Addressing EU legislative measures, the CJEU adopted important decisions with regard to the lawfulness and proportionality of data processing in the light of Articles 7 and 8 CFR. On the basis of these rights, the CJEU declared in 2006 and 2017 bilateral agreements between the EU and third states on the transfer of passenger data unlawful and in 2014 annulled the Data Retention Directive on the basis of which telecom providers were obliged to transfer data on their customers to EU law enforcement authorities.[58] Applying a stringent test to scrutinize EU instruments on the basis of these fundamental rights, assessing both their necessity

---

53 *Rechnungshof v. Österreichischer Rundfunk and Others* Joint Affairs C-465/00, C-138/01 and C-139/01, 20 May 2003, ECR I-4989, ss 71–83 and *Digital Rights Ireland*, 8 Apr. 2014 C-293/12, paras 35 and 55, referring to *S. and Marper v. UK* case and *M.K. v. France*, 18 Apr. 2013, no. 19522/09.

54 Preambles 71, 75 and 85 of the GDPR and preambles 23, 38, 51 and 61, and Art. 11(3) LED.

55 CJEU 16 Dec. 2008, C-524/06 (*Huber v. Germany*).

56 *See also* R. Gellert et al., *A Comparative Analysis of Anti-Discrimination Legislations and Data Protection Legislations*, in *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases* 61–89 (B. Custers et al. eds, Berlin/Heidelberg: Springer-Verlag 2013).

57 As provided in Art. 53 CFR, the level protection of the CFR will not go below the standards of the ECHR. These standards include the explanation of the ECHR in the case-law of the ECtHR.

58 *See* CJEU *EP v. Council*, Joined Cases C-317/04 and C-318/04, 30 May 2006, and the CJEU Opinion 1/15 of 26 July 2017, respectively C-293/12 *(Digital Rights Ireland Ltd)* 8 Apr. 2014, paras 57–68.

and proportionality, the CJEU provided in these judgments relevant criteria for the EU legislator when developing measures on data processing.[59] These criteria make clear that it is the obligation of the EU legislator to assess the necessity of the measure define a clear and limited purpose of the use of the personal information.[60] The criteria formulated by the CJEU in the *Digital Rights Ireland* case, to test whether data processing meets the criteria of 7 and 8 CFR, include the scope of data processing and whether its goal justifies the storage of data of an entire group of persons; the availability of prior review by court or independent body to assess which access for law enforcement purposes is strictly necessary; the availability of specific limits with regard to authorities having access to data and their subsequent use; and finally, the availability of time limits, restricting the storage of data to what is strictly necessary.[61]

Relevant criteria can be deduced as well from the judgment *Schwarz v. Bochum* in which the CJEU found that the Regulation 2252/2004 on the storage of biometrics in the EU passport did not involve a violation of Articles 7 and 8 CFR.[62] The CJEU based this conclusion on the following criteria assessing the necessity and proportionality of the provided storage and use of biometrics as provided in the Regulation. First, the CJEU found this only concerned a limited number of fingerprints, in combination of the facial recognition. Second, the CJEU underlined that the storage of biometric data at stake, was only for limited purposes, namely the verification of the authenticity of the passport and the identification of its owner. Third, while recognizing that fingerprints generally have a specific role in the field of criminal investigations, the CJEU explicitly found that on the basis of the Regulation at stake, the data would not be used for other purposes than preventing irregular migration of individuals to the EU territory. Finally, the CJEU held that Regulation 2252/2004 did not provide for the central storage of the collected fingerprints, as these would only be stored in the travel document which remains in the exclusive possession of the owner.[63] In a judgment of 9 October 2019, the CJEU answered preliminary questions from a Dutch court on whether the central storage of ten fingerprints and facial images of Turkish nationals at the national level, is in breach with the stand-still clause of the

---

59 *See also* on the implications of the CJEU's case-law: Irena Nesterova, *Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards*. European Society of International Law (ESIL) Conference Paper No. 11/2016 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2911999&download=yes.

60 EDPS, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (11 Apr. 2017).

61 *See also* CJEU C-362/14, *Schrems v. Data Protection Commissioner*, 6 Oct. 2015, paras 93–93, 98 and C-203/15 21 Dec. 2016 (*Tele2 Sverige AB Watson*) dealing with the E-Privacy directive.

62 CJEU 17 Oct. 2013, C-291/12 (*Schwarz v. Bochum*).

63 *See* paras 48, 55–56, 59 and 60–61.

EU-Turkey association agreements, also considering their rights protected in Articles 7 and 8 CFR.[64] While affirming this storage is a new restriction within the meaning of the association agreements, the CJEU held that it must be considered as justified by the objective of preventing and combating identity and document fraud. It is unclear why the CJEU did not address the question submitted by the national court on the use for law enforcement purposes in its overall assessment. Furthermore, it is regrettable that the referring court refused to submit a question on the possible discriminatory effect of this data processing. Even if it is disappointing that the CJEU seems more lenient in assessing the necessity and proportionality of the storage of (biometric) data of Turkish migrants by the Dutch administration, one might argue that the relevancy of this judgment is limited to its specific context. Whereas the CJEU did substantiate its conclusions by referring to the VIS and the Regulation on interoperability as 'EU examples' in this case, the CJEU has not been asked to address the overall use and effects (and thus necessity and proportionality) of EU large-scale databases. This remains a challenge for national courts.

It is not possible to assess the necessity and proportionality of each of the data processing measures described in this contribution. However, taking into account the aforementioned criteria, it must be questioned whether they will meet the test of the CJEU. As submitted by the FRA and EDPS when dealing with different of the aforementioned proposals, their added value and thus necessity generally have been insufficiently substantiated. Furthermore, the proportionality of the aforementioned measures, including the centralized storage of biometric data to be used for multiple purposes, seems even more difficult to prove, considering the criteria of the CJEU.

### 4.2 Purpose limitation

Reconsidering the principle of purpose limitation, it is important to emphasize that its goal or function is literally 'limitation' of the purposes for which personal data may be used. This means that 'specification' or definition of these purposes by contract or law does not offer sufficient protection.[65] This aspect of purpose limitation has been watered down in Article 6 GDPR providing that processing of personal data shall only be lawful for the grounds specified in Article 6. The definition of these grounds allows for a wide interpretation of 'purpose' of data

[64] CJEU 9 Oct. 2019, C-70/18 (*A,B,P*).

[65] Evelien Brouwer, *Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation*, in The Eclipse of Legality Principle in the European Union 279–294 (Leonard Besselink, Frans Pennings & Sacha Prechal eds, Alphen aan de Rijn: Kluwer Law International 2011).

processing, including the performance of a contract to which the data subject is a party, when this is necessary to comply with the legal obligations to which the data controller is subject, to protect the vital interest of the data subject or another natural person, and specifically relevant to our topic, if 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. Furthermore, Article 10 GDPR provides that data processing relating to criminal convictions and offences 'or related security measures' may only be carried out 'under the control of official authority' or when the processing is authorized by EU or national law providing for 'appropriate safeguards for the rights and freedoms of data subjects'. The GDPR thus provides a formal rather than a material interpretation of purpose limitation which does not seem in line with the criteria of the CJEU.

But even if one addresses the meaning of 'purpose specification', reflecting the necessity of legality and transparency of data processing, the aforementioned measures are difficult to reconcile with this principle of data protection. The extensive number of instruments dealing with data processing, with each their own set of data protection rules, in combination with the general rules in the GDPR and the Data Protection Directive, does not result in a very transparent legal framework. As underlined by the EDPS in the aforementioned Opinion 4/2018, the interoperability regulations only add another layer to the complexity of practices and laws of existing data systems. This complexity of rules triggers further questions on accountability and liability with regard to incorrect or unlawful data processing. If more databases and users are involved, it will be hard for individuals to understand which particular law applies and which state or organization should be addressed with regard to using their rights to access, correction or deletion of data, and right to legal remedies.

### 4.3 Prohibition of automated decision-making

The principle of prohibition of automated decision making is included in Article 22 GDPR and Article 11 Directive 2016/680. These provisions generally prohibit decision-making solely based on automated processing, including profiling, which produces 'adverse legal effects concerning the data subject or significantly affects him or her'.[66] This prohibition is not absolute. According to 22 (2) GDPR and Article 11 of the Directive automated decision-making is allowed if necessary for

[66] Articles 4 GDPR and 3 Directive 2016/680 define 'profiling' as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

performing a contract between data subject and data controller, or authorized by national or EU law, laying down 'suitable measures to safeguard data subject's rights and freedoms and legitimate interests or this is based on the explicit consent of the data subject. These suitable measures at least include the right of the data subject to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

As we have seen, the aforementioned data tools will be used for decisions or actions with direct implications for third-country nationals. Their request for visa, entry, or travel authorization may be refused and their residence status withdrawn on the basis of profiling, data sharing or the comparison of databases. In the aforementioned *Schwarz v. Bochum* the CJEU explicitly dealt with the risk of automated decision-making. Dealing with the claim of the applicant, that biometric data may be unreliable, the CJEU stressed that the use of the biometric passport will not lead to an automatic refusal of entrance. According to the CJEU, recognizing 'that the use of fingerprints as a means of ascertaining identity may, on an exceptional basis, lead to authorised persons being rejected by mistake', a mismatch between the fingerprints of the holder of a passport and the data in that document 'does not mean that the person concerned will automatically be refused entry to the European Union'. Interestingly, referring to Article 4(3) of Regulation 2252/2004, the CJEU observed that a 'mismatch of that kind will simply draw the competent authorities' attention to the person concerned and will result in a more detailed check of that person in order definitively to establish his identity'.[67] Indeed, also with regard to third-country nationals, the use of the aforementioned data systems often may 'simply' result in additional checks on their identity. However, considering the content of the aforementioned legislation and powers granted to the national authorities, the data stored in the large-scale databases will have a much wider impact for third-country nationals. Their rights to enter or to remain in the EU territory will depend on records stored into these databases and on risk assessments based on that information.

## 5 CLOSING REMARKS

In 2010, Simitis made the remark that despite the European Commission's explicitly stated willingness to comply with the European Charter of Fundamental Rights, this 'has not stopped the Commission from adopting regulations that openly contravene its duty to restrict all data uses to information needed for a precisely determined purpose'.[68] As we have seen in this contribution, the

[67] C-291/12, *Schwarz v. Bochum*, point 44.
[68] Spiros Simitis, *Privacy – An Endless Debate?*, 89(6) Cal. L. Rev., Art. 7 (Dec. 2010).

Commission developed in a relatively short period different measures, involving the large-scale registration of data on third-country nationals and extending the purposes and content of existing data systems. Aside from the increasing use of biometrics facilitating the possibility to check different data systems, large-scale databases initially set up for migration purposes, have turned into general investigation tools. Tools which are designed for external border controls, but may be used inside the territory for security and police checks as well. In its case-law, the CJEU formulated relevant criteria on the basis of the right to data protection, limiting the centralized storage of personal information, especially when this includes biometric data and involves the accessibility for law enforcement purposes. Whereas the purpose limitation provisions and the principle of automated-decision making in the GDPR and Directive 2016/680 allow for deviations, their essence must be observed. Considering the scope and implied risks of the described data systems, the conclusion that both the essence and non-discriminatory approach of data protection have been abandoned for third-country nationals, seems not too far-fetched. The question is only, when will the first claim of violation be brought before the European Courts?